Notice of Allowability	Application No.	Applicant(s)	
	09/712,505	DRISCOLL, KEVIN R.	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *4/4/07*.

2. ☒ The allowed claim(s) is/are *1-43*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Reasons for Allowance

1. Claims 1-43 are allowable for the following features: "in a stream cipher..."receiving a first plaintext binary data sequence and the encryption keystream and performing a first set of two non-associative operations on the first plaintext binary data sequence and the encryption keystream to provide a ciphertext binary data sequence", receiving the ciphertext binary data sequence and the data keystream and performing a second set of two non-associative operations on the ciphertext binary data sequence and the decryption keystream to provide a second plaintext binary data sequence identical to the first plaintext binary data sequence"; "receiving a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence", 'combining the plaintext binary data sequence and the encryption keystream with two non-associative operations to provide a ciphertext binary data sequence".

2. An example of prior art that fails to disclose or suggest, "in a stream cipher..."receiving a first plaintext binary data sequence and the encryption keystream and performing a first set of two non-associative operations on the first plaintext binary data sequence and the encryption keystream to provide a ciphertext binary data sequence", receiving the ciphertext binary data sequence and the data keystream and performing a second set of two non-associative operations on the ciphertext binary data sequence and the decryption keystream to provide a second plaintext binary data sequence identical to the first plaintext binary data sequence"; "receiving a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data

sequence", "combining the plaintext binary data sequence and the encryption keystream with two non-associative operations to provide a ciphertext binary data sequence", is Ritter. Ritter does not teach or suggest combining a "first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence". In contrast, Ritter discloses a dynamic substitution combiner and extractor. A plaintext value on input is transformed by substitution into a ciphertext value output. A ciphertext value on input is transformed by substitution into the original plaintext value on output. Ritter teaches away from the present invention and claim language that states "a stream cipher". Ritter teaches that a stream cipher which uses exclusive-OR is susceptible to attack.

3. An example of prior art that fails to disclose or suggest, "in a stream cipher..."receiving a first plaintext binary data sequence and the encryption keystream and performing a first set of two non-associative operations on the first plaintext binary data sequence and the encryption keystream to provide a ciphertext binary data sequence", receiving the ciphertext binary data sequence and the data keystream and performing a second set of two non-associative operations on the ciphertext binary data sequence and the decryption keystream to provide a second plaintext binary data sequence identical to the first plaintext binary data sequence"; "receiving a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence", "combining the plaintext binary data sequence and the encryption keystream with two non-associative operations to provide a ciphertext binary data sequence", is Coppersmith. Coppersmith discloses s symmetric block cipher cryptosystem, which is in contrast to the claim

limitation that claims a "stream cipher". Coppersmith discloses the category of symmetric encryption systems can be further subdivide into those which operate on fixed sized blocks of data(block cipher) and those which operate on arbitrary length streams of data(stream ciphers). In block cipher cryptosystems, if one fixed common private-key is employed to encipher different occurrences of a particular plaintext block, all of these occurrences are encrypted into identical corresponding ciphertext blocks. By contrast, in stream cipher cryptosystems, the plaintext is typically encrypted on a bit-by-bit or word-by-word basis using a stateful transform that evolves as the encryption progresses.

4. Another example of prior art that fails to disclose or suggest, "in a stream cipher..."receiving a first plaintext binary data sequence and the encryption keystream and performing a first set of two non-associative operations on the first plaintext binary data sequence and the encryption keystream to provide a ciphertext binary data sequence", receiving the ciphertext binary data sequence and the data keystream and performing a second set of two non-associative operations on the ciphertext binary data sequence and the decryption keystream to provide a second plaintext binary data sequence identical to the first plaintext binary data sequence"; "receiving a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence", "combining the plaintext binary data sequence and the encryption keystream with two non-associative operations to provide a ciphertext binary data sequence", is Clapp. Clapp discloses a pseudo-random bitstream, which can be combined with a datastream to be encoded over a line, for example using an exclusive-OR operations in a combiner, to produce a resulting bitstream over a line for transmission to a decoding receiver.

Clapp discloses a pseudo-random number generator that is a finite state machine having two component types, w-bit non-linear combiner and a plurality of w-bit registers. The non-linear combiner and the registers are connected together to create a data path subject. Clapp is in contrast, to claim limitations that claim, "in a stream cipher..."receiving a first plaintext binary data sequence and the encryption keystream and performing a first set of two non-associative operations on the first plaintext binary data sequence and the encryption keystream to provide a ciphertext binary data sequence", receiving the ciphertext binary data sequence and the data keystream and performing a second set of two non-associative operations on the ciphertext binary data sequence and the decryption keystream to provide a second plaintext binary data sequence identical to the first plaintext binary data sequence"; "receiving a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence", "combining the plaintext binary data sequence and the encryption keystream with two non-associative operations to provide a ciphertext binary data sequence".

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

June 5, 2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100